$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$e_k \equiv e \pmod{(p_k - 1)},$$

where e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said subtasks to determine results C_1, C_2 ... C_k,

combining said results of said subtasks in accordance with a fast recursive combining process to produce said ciphertext word signal C whereby,

$$Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n$$

$$2 \le i \le k, \text{ and}$$

$$C = Y_k,\ Y_1 = C_1, \text{ and } w_i = \prod_{j<i} p_j$$

whereby said step of encoding is accelerated.

15. (Three Times Amended) A method for establishing cryptographic communications that are backwards compatible with preexisting public key transformation schemes, comprising the steps of:

decoding a ciphertext word C to a message word M, wherein M corresponds to a number representative of a message and wherein,

$$0 \le M \le n-1$$

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2, and p_1, p_2, ..., p_k are distinct random prime numbers, C is a number representative of an

encoded form of message word M that is encoded by transforming said message word M to said ciphertext word C whereby,

$$C \equiv M^e \pmod{n},$$

and wherein e is a number relatively prime to (p_1-1), (p_2-1), …, and (p_k-1),

said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1)),$$

said decoding step including the steps of,

(i) defining a plurality of k sub-tasks in accordance with

$$M_1 \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2 \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv C_k^{d_k} \pmod{p_k},$$

where

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

(ii) solving said sub-tasks to determine results $M_1, M_2, \ldots M_k$, and

(iii) combining said results of said subtasks in accordance with a fast recursive combining process to produce said message word M in accordance with,

$$Y_i \equiv Y_{i-1} + [(M_i - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n$$

where $2 \leq i \leq k$, and

$$M = Y_k, Y_1 = M_1, \text{and } w_i = \prod_{j<i} p_j$$

whereby said step of decoding is accelerated.

16. (Three Times Amended) A cyptographic communications system for establishing communications that are backwards compatible with preexisting public key transformation schemes, comprising:

a communication medium;

encoding means coupled to said communication medium and adapted for transforming a transmit message word M to a ciphertext word C and for transmitting said ciphertext word C on said medium, where M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$ where n is a composite number of the form

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$,

where k is an integer greater than 2 and $p_1, p_2, \ldots p_k$ are distinct random prime numbers, and where C corresponds to a number representative of an enciphered form of said message, and corresponds to

$C \equiv M^e \pmod{n}$,

where e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

decoding means coupled to said communication medium and adapted for receiving C via said medium and for transforming C to a receive message word M' where M' corresponds to a number representative of a deciphered form of C, said decoding means being operative to perform a decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1)),$$

said decryption process including the steps of

(i) defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

where,

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)},$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2}, \text{ and}$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

(ii) solving said sub-tasks to determine results M_1', M_2', ... M_k', and

(iii) combining said results of said subtasks by a fast recursive combining process to produce said receive message word M' in accordance with

$$Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1})\ (w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n$$

where $2 \leq i \leq k$ and

$$M' = Y_k,\ Y_1 = M_1,\ \text{and}\ w_i = \prod_{j<i} p_j,$$

wherein M'=M.

---

17. (Twice Amended) A method for establishing cryptographic communications that are backwards compatible with preexisting public key transformation schemes, comprising the steps of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$$0 \leq M \leq n-1,$$

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, C is a number representative of an encoded form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C, whereby

$$C \equiv M^e \pmod{n},$$

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

decoding said ciphertext word C to a receive message word M', said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1)),$$

said decoding step including the further steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', wherein M'=M.

---

22. (Twice Amended) A cyptographic communications system for establishing communications that are backwards compatible with preexisting public key transformation schemes, comprising:

a communication medium;

encoding means coupled to said communication medium and adapted for transforming a transmit message word M to a ciphertext word C and for transmitting said ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$, wherein n is a composite number of the form,

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$

wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein said ciphertext word C corresponds to a number representative of an enciphered form of said message and corresponds to

$C \equiv M^e \pmod{n}$,

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

decoding means communicatively coupled with said communication medium for receiving said ciphertext word C via said medium, said decoding means being operative to perform a decryption process for transforming said ciphertext word C to a receive message word M', wherein M' corresponds to a number representative of a deciphered form of C, said decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1)),$$

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)},$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M'

whereby M'=M.

27. (Twice Amended) A method for establishing cryptographic communications that are backwards compatible with preexisting public key transformation schemes, comprising the step of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message, and

$0 \le M \le n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, wherein said step of encoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$e_k \equiv e \pmod{(p_k - 1)},$$

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

32. (Twice Amended) A cyptographic communications system for establishing communications that are backwards compatible with preexisting public key transformation schemes, comprising:

a communication medium;

encoding means coupled to said communication medium and operative to transform a transmit message word M to a ciphertext word C, and to transmit said ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ wherein k is an integer greater than 2 and p_1, p_2, ..., p_k, are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, said encoding means being operative to transform said transmit message word M to said ciphertext word C by performing an encoding process comprising the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$e_1 \equiv e \pmod{(p_1 - 1)}$,

$e_2 \equiv e \pmod{(p_2 - 1)}$, and

$\vdots$

$e_k \equiv e \pmod{(p_k - 1)}$,

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

37. (Twice Amended) A method for establishing cryptographic communications that are backwards compatible with preexisting public key transformation schemes, comprising the steps of:

decoding a ciphertext word C to a message word M, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n-1$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, C is a number representative of an encoded form of message word M that is encoded by transforming said message word M to said ciphertext word C whereby

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1);

said decoding step being performed using a decryption exponent d that is defined by

$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1))$,

wherein said step of decoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$M_1 \equiv C_1^{d_1} \pmod{p_1}$,

$M_2 \equiv C_2^{d_2} \pmod{p_2}$,

$\vdots$

$M_k \equiv C_k^{d_k} \pmod{p_k}$,

wherein

$C_1 \equiv C \pmod{p_1}$,

$C_2 \equiv C \pmod{p_2}$,

⋮

$C_k \equiv C \pmod{p_k}$,

$d_1 \equiv d \pmod{(p_1 - 1)}$,

$d_2 \equiv d \pmod{(p_2 - 1)}$, and

⋮

$d_k \equiv d \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results $M_1, M_2, \ldots M_k$, and

combining said results of said sub-tasks to produce said message word M.

---

42. (Twice Amended) A cyptographic communications system for establishing communications that are backwards compatible with preexisting public key transformation schemes, comprising:

a communication medium;

communicatively coupled with said communication medium for receiving a ciphertext word C via said medium, and being operative to transform said ciphertext word C to a receive message word M', wherein a message M corresponds to a number representative of a message and wherein,

$0 \leq M \leq n-1$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein said ciphertext word C is a number representative of an encoded form of said message word M that is encoded by transforming M to said ciphertext word C whereby,

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), …, and (p_k-1);

said decoding means being operative to perform a decryption process using a decryption exponent d that is defined by

$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1))$,

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with,

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein,

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', whereby M'=M.

47. (Twice Amended) A method for generating a digital signature that is backwards compatible with preexisting public key transformation schemes, comprising the step of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message, and

$0 \le M \le n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of message word M, wherein

$C \equiv M^d \pmod{n}$, and

wherein said step of signing includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

wherein d is defined by

$$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1)), \text{ and}$$

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

52. (Twice Amended) A digital signature generation system that is backwards compatible with preexisting public key transformation schemes, comprising:

a communication medium;

digital signature generating means coupled to said communication medium and operative to transform a transmit message word M to a signed ciphertext word C, and to transmit said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$, are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of said message word M, wherein

$C \equiv M^d \pmod{n}$,

said digital signature generating means being operative to transform said transmit message word M to said signed ciphertext word C by performing a digital signature generating process comprising the steps of,

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where,

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

wherein d is defined by,

$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results $C_1, C_2, \ldots C_k$, and

combining said results of said sub-tasks to produce said signed ciphertext word C.

57. (Twice Amended) A digital signature process that is backwards compatible with preexisting public key transformation schemes, comprising the steps of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$$0 \le M \le n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, C is a number representative of a signed form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C whereby,

$$C \equiv M^d \pmod{n},$$

wherein d is defined by

$$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1)), \text{ and}$$

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

verifying said ciphertext word C to a receive message word M' by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$e_k \equiv e \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', whereby M'=M.

62. (Twice Amended) A digital signature system that is backwards compatible with preexisting public key transformation schemes, comprising:

a communication medium;

digital signature generating means coupled to said communication medium and adapted for transforming a message word M to a signed ciphertext word C and for transmitting said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$, wherein n is a composite number of the form

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$,

wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein said signed ciphertext word C corresponds to a number representative of a signed form of said message word M and corresponds to

$C \equiv M^d \pmod{n}$,

wherein d is defined by

$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

digital signature verification means communicatively coupled with said communication medium for receiving said signed ciphertext word C via said medium, and being operative to verify said signed ciphertext word C by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

wherein

$C_1 \equiv C \pmod{p_1}$,

$C_2 \equiv C \pmod{p_2}$,

⋮

$C_k \equiv C \pmod{p_k}$,

$e_1 \equiv e \pmod{(p_1 - 1)}$,

$e_2 \equiv e \pmod{(p_2 - 1)}$,

⋮

$e_k \equiv e \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M'

wherein M'=M.